UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA, Plaintiff, v. KRISTOPHER LEE DALLMANN, *et al.*, Defendants.	Case No. 2:22-cr-00030-RFB-DJA **ORDER**

I. INTRODUCTION

Before the Court is Defendant Kristopher Dallmann's Motion to Suppress. ECF No. 157. For the following reasons, the Motion to Suppress is denied.

II. PROCEDURAL AND FACTUAL BACKGROUND

On August 27, 2019, the indictment in this case was filed in the United States District Court for the Eastern District of Virginia. ECF No. 1. On February 3, 2022, the case was transferred to the United States District Court for the District of Nevada. Id. There are nineteen counts included in the indictment. The Government alleges that from about 2007 to 2017, Mr. Dallman, with the assistance of others, operated Jetflicks, an online, subscription-based service that permitted users to stream and download copyrighted television programs without the permission of the relevant copyright owners. The Defendant willfully reproduced tens of thousands of copyrighted television episodes and distributed the programs to individuals throughout the United States. The estimated harm to copyright owners was millions of dollars. Jetflicks operated similarly to Netflix, Hulu, and Amazon Prime Video. For a subscription fee as little as $9.99 per month, Jetflicks enabled its subscribers to watch an unlimited number of commercial-free television programs, often within days of the episodes' first airings. The company sought to make these programs available on a

variety of devices and platforms including Apple TV, Google Chromecast, and Roku. Jetflicks obtained television programs from other sites hosting infringing content. Jetflicks, at one point, claimed to offer more than 183,200 television episodes and have more than 37,000 subscribers.

On January 18, 2024, Mr. Dallmann submitted a Motion to Suppress. ECF No. 157.

III. LEGAL STANDARD

The Fourth Amendment protects the right of the people to be secure in their persons against unreasonable searches and seizures by the government. U.S. Const. amend. IV. A warrantless search is per se unreasonable under the Fourth Amendment, subject to only a "few specifically established and well-delineated exceptions." Katz v. United States, 389 U.S. 347, 357 (1967). Since the Fourth Amendment protects people not places, the "capacity to claim the protection of the Fourth Amendment depends ... upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." Minnesota v. Olson, 495 U.S. 91, 95 (1990).

The Fourth Amendment requires that a search warrant describe with particularity the "things to be seized." U.S. Const. amend. IV. Search warrants must be specific in both particularity and breadth. United States v. Towne, 997 F.2d 537, 544 (9th Cir. 1993). "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." Id. (citation and internal quotation marks omitted). Probable cause must exist to seize all the items of a particular type described in the warrant. United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986).

A search warrant is sufficiently particular if it "enable[s] the person conducting the search reasonably to identify the things authorized to be seized." United States v. Mann, 389 F.3d 869, 877 (9th Cir. 2004). "Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible. United States v. Lei Shi, 525 F.3d 709, 731 (9th Cir. 2008) (internal citations omitted).

A search warrant is not overbroad if its scope is supported by probable cause. United States v. SDI Future Health, Inc., 568 F.3d 684, 703 (9th Cir. 2009) ("The search and seizure of large

quantities of material is justified if the material is within the scope of the probable cause underlying the warrant.") (quoting United States v. Hayes, 794 F.2d 1348, 1355 (9th Cir. 1986)). When determining whether a warrant is overbroad, a court must consider: (1) whether probable cause existed to seize all items of a category described in the warrant, (2) whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not, and (3) whether the government could have described the items more particularly in light of the information available. United States v. Flores, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting United States v. Lei Shi, 525 F.3d 709, 731-32 (9th Cir. 2008)).

Unique challenges arise when executing search warrants on electronically stored information. That is because "[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents[.]" Flores, 802 F.3d at 1044-45 (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176-77 (9th Cir. 2010)). Given those challenges, the federal rules provide for a two-step process wherein "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41(e)(2)(B) advisory committee note to 2009 amendment. The Ninth Circuit has adopted this two-step approached. See Flores, 802 F.3d at 1046; United States v. Pelayo, No. 21-30249, 2023 U.S. App. LEXIS 19624, 2023 WL 4858147, at *2 n.2 (9th Cir. July 31, 2023); United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013).

At the same time, courts have also recognized that the "nature of digital storage" creates "enormous" risks of authorizing "unbridled, exploratory search[es]" of electronically stored data. United States v. Galpin, 720 F.3d 436, 446-47 (2d Cir. 2013). Thus, while the Ninth Circuit has acknowledged that the "reality of over-seizing is an inherent part of the electronic search process," it has also emphasized the need for a "greater vigilance on the part of judicial officers" in balancing the needs of law enforcement and the privacy rights of the people. CDT, 621 F.3d at 1177; see also Schesso, 730 F.3d at 1042 ("[L]aw enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence.").

///

///

IV. DISCUSSION

Defendant Kristopher Dallmann asserts that the government unlawfully seized substantial portions of Mr. Dallmann's digital information through a defective search warrant. The Court addresses the defendant's arguments, in turn.

a. Probable Cause Supporting Search Warrant

Mr. Dallmann argues that the search warrant application for five separate email accounts failed to establish a nexus between the accounts and probable cause of any criminal activity.

i. Legal Standard

The Fourth Amendment provides that a warrant may be issued only upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. U.S. Const. amend. IV. In order to comply with this constitutional requirement, the warrant must be issued by a neutral and detached magistrate, supported by probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense, and describe the things to be seized and the place to be searched with particularity. United States v. Artis, 919 F.3d 1123, 1129 (9th Cir. 2019) (quoting Dalia v. United States, 441 U.S. 238, 255 (1979)) (internal quotation marks omitted).

The determination of whether probable cause exists is a practical, common-sense decision made in light of the totality of the circumstances. Illinois v. Gates, 462 U.S. 213, 238 (1983). A search warrant affidavit will demonstrate probable cause "if, under the totality of the circumstances, it reveals a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Celestine, 324 F.3d 1095, 1102 (9th Cir. 2003). Probable cause "is not a high bar." Kaley v. United States, 571 U.S. 320, 338 (2014)). Only a fair probability is needed, and not a certainty, that evidence of crime or contraband will be found. See Gates, 462 U.S. 213 at 235. In determining whether a search warrant was based upon probable cause, the district court is limited to the information and circumstances contained within the four corners of the underlying affidavit. United States v. Stanert, 762 F.2d 775, 778, amended on other grounds, 769 F.2d 1410 (9th Cir. 1985). An affidavit need only show facts adequate to support a finding of probable cause. United States v. Johns, 948 F.2d 599, 606 (9th Cir. 1991).

In the case of a search warrant, "[a] magistrate judge's finding of probable cause is entitled to great deference and [the] court will not find a search warrant invalid if the magistrate judge had a substantial basis for concluding that the supporting affidavit established probable cause." United States v. Clark, 31 F.3d 831, 834 (9th Cir. 1994).

ii. Mr. Dallmann's Personal Email Account

The Defendant argues that there is no nexus between the Jetflicks email account – kristopher.dallmann@gmail.com – and criminal activity. The affidavit in support of the warrant was written by FBI Special Agent ("SA") Chase. It describes the relevant circumstances surrounding the search.

The Court makes the following findings based upon the record. The FBI began investigating Jetflicks for copyright infringement starting in or around September 2015. This investigation led the bureau to identify Kristopher Dallmann as the owner and operator of Jetflicks. Records obtained from Google indicated that Mr. Dallmann's email address – Kristohper.Dallmann@gmail.com – was linked by electronic cookies to the Jetflicks email account – Krisoph@jetflicks.com. The affidavit explains that a "cookie" is a small amount of data generated by a website and saved by a web browser. It can allow a party to identify other accounts accessed from the same computer; accounts whose subscriber information includes the same phone number or email address; and accounts where the same IP addresses were used to create or access the account in the same timeframe.

Additionally, other records indicated that his personal email address: communicated or was copied on emails with Jetflicks email accounts; and was associated with the Google Analytics account connected to Jetflicks. Mr. Dallmann's Google+ page associated with his personal email account was also used to advertise Jetflicks business information. Finally, Mr. Dallmann's personal email account along with several Jetflicks email accounts were linked to his phone number. The email address was included in business conversations associated with Jetflicks and was used to manage the media advertising of the company. Under the totality of the circumstances, the Court finds that the search warrant reveals a fair probability that evidence of a crime related to the operation of Jetflicks would be found within the contents of Mr. Dallmann's personal email

account. See United States v. Celestine, 324 F.3d 1095, 1102 (9th Cir. 2003).

The Defendant takes particular umbrage to the language of the affidavit. He argues the affidavit provides vague, conclusory reason speculating that it is "reasonable to believe" that Mr. Dallmann used his personal email account in connection with the operation of Jetflicks, and this assertion that something is reasonable to believe falls short of probable cause.

The Ninth Circuit has long held that affiants seeking a warrant may state conclusions based on training and experience without having to detail that experience. United States v. Garay, 938 F.3d 1108, 1113 (9th Cir. 2019). Additionally, affiants seeking a warrant may state conclusions based on training and experience without having to detail that experience. See, e.g., United States v. Hendershot, 614 F.2d 648, 654 (9th Cir. 1980) (finding that affiant's conclusion "based on [his] experience from prior bank robbery investigations" was proper; emphasizing that "[i]t is not necessary to detail that experience to determine that the conclusion is not capricious" (internal quotation marks omitted)). Here, SA Chase detailed his professional training and experience, including his specialized training on fraud and complex financial crimes. The Court does not find the Defendant's reasoning to be a sufficient basis to invalidate the search warrant.

Accordingly, the Court finds that there was sufficient probable cause to support the warrant with respect to this email account.

iii. The Jetflicks Email Account

The Defendant argues that there is no nexus between the Jetflicks email account – jetflicksmobile@gmail.com – and criminal activity. The affidavit states that this account was listed as the developer for Jetflicks mobile device software applications. Additionally, the account name is "Jetflicks Support;" the recovery email address for this account is a Jetflicks email address; and the associated phone number belongs to the Defendant. Under the totality of the circumstances, the Court finds that the search warrant reveals a fair probability that evidence of a crime related to the operation of Jetflicks would be found within the contents of Mr. Dallmann's personal email account. See United States v. Celestine, 324 F.3d 1095, 1102 (9th Cir. 2003). There was a connection to the operation of Jetflicks through the use of this email account as it was the account listed as the developer of the Jetflicks mobile application. This evidence presents a fair probability

that evidence of the alleged crime would be found within the contents of this account. See Gates, 462 U.S. 213 at 235. Accordingly, the Court finds that there was sufficient evidence to support the warrant with regard to this email account.

iv. Mr. Dallmann's Jetflicks Email Account

The Defendant asserts that there is no nexus between Mr. Dallmann's Jetflicks email account – kristoph@jetflicks.com – and criminal activity. The affidavit asserts that this account was used to purchase the domain names for the Jetflicks websites, and create various social media accounts for Jetflicks to advertise and promote the company. As the email account used to purchase the website domain that housed Jetflicks, there is a fair probability that evidence of the alleged crime would be found within the contents of this account. See Gates, 462 U.S. 213 at 235. Accordingly, the Court finds that there was sufficient evidence to support the warrant with regard to this email account.

v. Mr. Dallmann's Alternate Jetflicks Email Account

The Defendant argues that there is no nexus between Mr. Dallmann's alternate Jetflicks email account – kris@jetflicks.com – and criminal activity. The supporting affidavit states that this email address was used to make reoccurring payments to Jetflicks on behalf of the Defendant. It was also listed on credit applications by the Defendant for the purchase of multiple automobiles with "Jetflicks, LLC" listed as the Defendant's employer and as the recovery email for jetflicksmobile@gmail.com. It must also be reiterated here that the entire Jetflicks enterprise was alleged to be an ongoing criminal enterprise so an information related to the maintenance and operation of the business could be evidence of a crime.

Probable cause "is not a high bar." Kaley v. United States, 571 U.S. 320, 338 (2014)). Only a fair probability is needed, and not a certainty, that evidence of crime or contraband will be found. See Gates, 462 U.S. 213 at 235. The Court finds that there are sufficient connections between Jetflicks and the email account, especially that the account was used to make payments to Jetflicks on behalf of the Defendant, to establish probable cause. Accordingly, the Court finds that there was sufficient evidence to support the warrant with regard to this email account.

///

vi. The Jetflicks Support Email Account

The Defendant asserts that there is no nexus between the Jetflicks customer support service email account – support@jetflicks.com – and criminal activity. This email address is listed on the Jetflicks website for support requests. An individual identified as a member of Jetflicks' customer support team responded and indicated that he assisted with managing content available on the Jetflicks website. This is also the email address listed as the point of contact for Jetflicks. Under the totality of the circumstances, this evidence shows that this email account was used for conducting official yet illegal Jetflicks business. It demonstrates a fair probability that evidence of a crime would be found in the contents of the email account. See United States v. Celestine, 324 F.3d 1095, 1102 (9th Cir. 2003). Accordingly, the Court finds that there was sufficient evidence to support the warrant with regard to this email account.

b. Constitutional Specificity of Search Warrant

Mr. Dallmann argues that the search warrant was not sufficiently specific. The Constitution mandates that a warrant "particularly describe[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Fourth Amendment's specificity requirement prevents officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized. United States v. Adjani, 452 F.3d 1140, 1147 (9th Cir. 2006) (citations omitted).

The Ninth Circuit has determined that specificity is distinguished by two aspects – particularity and breadth. The Court addresses both aspects, in turn.

i. Legal Standard – Particularity

Particularity is the requirement that the warrant must clearly state what is sought. United States v. SDI Future Health, Inc., 568 F.3d 684, 702 (9th Cir. 2009) (citing In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 856-57 (9th Cir. 1991)). Particularity means that "the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize." Id. The description must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized. Id. (citing United States v. Smith, 424 F.3d 992, 1004 (9th Cir. 2005)). Warrants which describe generic categories

of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible. Id.

In determining whether a warrant is sufficiently particular, courts consider one or more of the following factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006).

ii. Discussion

First, the Court has determined that there was sufficient probable cause to search the contents of Mr. Dallmann's email accounts. Second, the Court finds that "the warrant objectively described the items to be searched and seized with adequate specificity and sufficiently restricted the discretion of agents executing the search." Id. The Ninth Circuit has emphasized a focus on tying the documents sought to the crimes that are alleged. Id. Similarly as in Adjani, the warrant limits the search for evidence of a specific crime. Id. Here, the different categories of information to be seized specifically relates to the participants in and operation of the alleged copyright scheme. The search warrant identifies the specific crime and the records and documents requested are related to that crime. Additionally, "the extensive statement of probable cause in the affidavit detailed the alleged crime and [the Defendant's] unlawful scheme." Id.

Third, "the government described the items to be searched and seized as particularly as could be reasonably expected given the nature of the crime and the evidence it then possessed." Id. A search warrant need only be specific, rather than reasonably detailed. Id. In Adjani, the warrant provided the precise identity and nature of the items to be seized. The warrant instructed agents to search for documents reflecting communications with three individuals or other employees of a specific company; and authorized seizure of "any" evidence of travel but provided a specific, though not exhaustive, list of possible documents that fell within this category and temporally restricted the breadth of the search. Id. Similarly, the search warrant here authorized

agents to search for documents associated with the email accounts of alleged members of the copyright scheme; "all" Google Map data; among other items of information. The Ninth Circuit recognizes the heightened specificity concerns in the computer context, but has found that to require a pin-pointed computer search, restricting the search to an email program or to specific search terms, will likely fail to cast a sufficiently wide net to capture the evidence sought. Id. at 1149-50. With the information already in the government's possession, the search warrant properly described the information sought.

Accordingly, the Court finds that the search warrant was sufficiently particular.

iii. Legal Standard – Breadth

Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based. United States v. SDI Future Health, Inc., 568 F.3d 684, 702 (9th Cir. 2009). The concept of breadth may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant. In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 857 (9th Cir. 1991). Probable cause must exist to seize all the items of a particular type described in the warrant. Id. (citing United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)).

Courts determining whether a warrant is overbroad consider: (1) whether probable cause existed to seize all items of a category described in the warrant; (2) whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not; and (3) whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued. United States v. Shi, 525 F.3d 709, 731-32 (9th Cir. 2008) (citing United States v. Noushfar, 78 F.3d 1442, 1447 (9th Cir. 1996), amended, 140 F.3d 1244 (9th Cir. 1998)).

iv. Discussion

In United States v. Flores, the Ninth Circuit considered a similar situation where the search of a defendant's social media account was challenged. 802 F.3d 1028 (9th Cir. 2015). In considering the first two Shi factors whether there was probable cause and whether the warrant set forth objective standards, the panel held that it was not overbroad. This was because only searches

associated with the defendant's name and email address were allowed, and only evidence associated with violations of the relevant statutes were authorized for seizure. The Defendant complained that all 11,000 pages of data in his account were authorized for search and seizure while only 100 pages were truly responsive. In addressing the third Shi factor, the Ninth Circuit rejected the argument that the government should have narrowed its search. It determined that "over-seizing" is an accepted reality in electronic searching because "[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents." Id. at 1028 (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam)).

Similarly in Adjani, the defendant argued that a search warrant focused on his electronic information was a wholesale search of the contents of all emails purportedly looking for evidence reflecting communications with involved individuals and could have been less invasive. 452 F.3d at 1149. The court found that "[a]voiding that kind of specificity and limitation was not unreasonable under the circumstances." Id. at 1149-50. To require a "pin-pointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought." Id. at 1150.

First, as the Court has addressed, there was probable cause to search the contents of Mr. Dallmann's email accounts. Second, as in Flores and Adjani, the search warrant covers evidence related to the email accounts of email accounts involved in the alleged wrongdoing. While this does constitute a potentially significant amount of information, a pin-point search may have failed to cast a sufficiently wide net to identify pertinent information. See Adjani, 452 F.3d at 1150. Third, here as in Adjani, the Court finds that the search warrant's broad language appropriate to cast a sufficiently wide net to capture evidence of the alleged digital copyright activity.

The Defendant also argues that the lack of a temporal limitation is particularly problematic. However, the Ninth Circuit has not definitely resolved whether a complete lack of temporal limitation on searches for electronic information are facially overbroad. See Flores, 802 F.3d at 1045 ("Ultimately we need not decide whether the warrant was overbroad for lack of temporal limit because even if it was, suppression of the evidence used at trial was not required. …

Therefore, even though the warrant had no temporal limit, the district court did not err in denying [the defendant's] motion to suppress"). Moreover, while the Defendant argues that the warrant should have included temporal limitations starting in October 2011 when Mr. Dallmann's personal email address account was created, the supporting affidavit identifies activity related to the organization of Jetflicks prior to this date. For example, the affidavit states that the Jetflicks domain was purchased as far back as 2008. The Court finds that the temporal limitation is not required and the timeframe identified by the Defendant would create a pinpoint that would prevent the government from acquiring relevant evidence. See Adjani, 452 F.3d at 450.

Accordingly, the Court finds that the search warrant is not overly broad. Hence, the warrant is sufficiently specific.

c. Unlawful Seizure

Mr. Dallmann asserts that the government unlawfully seized his email accounts when it directed Google to preserve his account data without probable cause or a search warrant.

The Stored Communications Act, 18 U.S.C. § 2703, at Section (f) requires a provider of wire or electronic communication services or a remote computing service to take necessary steps to preserve records and other evidence in its possession pending issuance of a court order or other process upon the request of a government entity. See 18 U.S.C. § 2703(f). The provider is required to retain the records for a period of ninety days. Id.

i. Preservation as Government Action

Mr. Dallmann argues that Google became a government action by preserving his digital information at the request of the FBI under §2703(f).

The Fourth Amendment regulates only governmental action; it does not protect against intrusive conduct by private individuals acting in a private capacity. United States v. Rosenow, 50 F.4th 715, 728 (9th Cir. 2022) (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)). A private search or seizure may implicate the Fourth Amendment where the private party acts "as an agent of the Government or with the participation or knowledge of any governmental official." Id. (quoting Jacobsen, 466 U.S. at 113 (internal quotation marks and citation omitted)). A defendant challenging a search conducted by a private party bears the burden of showing the search was

governmental action. Id. (quoting United States v. Young, 153 F.3d 1079, 1080 (9th Cir. 1998) (per curiam)). Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances. Id. (quoting Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614-15 (1989)).

The Ninth Circuit addressed a similar issue in United States v. Rosenow. 50 F.4th 715 (9th Cir. 2022). In that case, the defendant argued that federal regulation of electronic service provider searches and disclosures triggers the Fourth Amendment because the two relevant federal statutes authorized warrantless searches and required private parties to report evidence derived from those searches. The court found this argument unconvincing. The first statute, The Stored Communications Act, "did not authorize the service providers to do anything more than access information already contain on their servers." Id. at 730. The second statute, the Protect Our Children Act, only authorized mandatory searching, not mandatory reporting. Id.

Here, similarly as in Rosenow, the Government made a request for preservation pursuant to 18 U.S.C. § 2703(f). This statute "did not authorize the service providers to do anything more than access information already contain on their servers." Id. at 730. Google complied with a federal statute mandating preservation of records. Importantly, the Court finds that Google did not search the content of its records for evidence of a crime—as government agent would. It merely preserved existing records. The Ninth Circuit emphasized that a private actor does not become a government agent simply by complying with a mandatory reporting statute. Id. (referencing Mueller v. Auker, 700 F.3d 1180, 1191-92 (9th Cir. 2012)). Google would then not be a government agent by merely preserving information already in its possession.

The Court finds that Google was not a government agent, and the Defendant did not meet its burden of showing that the search was governmental action. See United States v. Rosenow, 50 F.4th 715, 728 (9th Cir. 2022). "[E]ven if the Fourth Amendment protects files stored with an [E]SP, the [E]SP can search through all of the stored files on its server and disclose them to the government without violating the Fourth Amendment." Id. (quoting Orin Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev.

1208, 1212 (2004)).

Hence, the Fourth Amendment was not implicated by Google's actions. Accordingly, the Court determines that the Government did not unlawfully seize Mr. Dallmann's email accounts through its preservation request.

d. Tainted Search Warrant

Mr. Dallmann asserts that the search warrants for his home independently lacked probable cause, lacked sufficient particularity, and was obtained through evidence tainted by other Fourth Amendment violations. The Court addresses each argument, in turn.

i. Lack of Probable Cause

The Defendant argues that SA Chase's supporting affidavit relied on his own suspicions and provided wholly conclusory statements which did not show a nexus between Mr. Dallman's residence and criminal activity. He also argues that the warrant had an indiscriminate sweep and far outstripped the police's proffered justification for search and seizure.

As explained previously in this order, the determination of whether probable cause exists is a practical, common-sense decision made in light of the totality of the circumstances. Illinois v. Gates, 462 U.S. 213, 238 (1983). A search warrant affidavit will demonstrate probable cause "if, under the totality of the circumstances, it reveals a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Celestine, 324 F.3d 1095, 1102 (9th Cir. 2003). Probable cause "is not a high bar." Kaley v. United States, 571 U.S. 320, 338 (2014)).

Here, SA Chase's affidavit sought a search warrant for two properties owned by Mr. Dallmann – one property at 2154 Tona Circle (the "2154 Tona Property") and one property at 2216 Tona Circle (the "2216 Tona Property"). The 2154 Tona Property was identified as the registered address for Jetflicks in records obtained from the Nevada Secretary of State and as the address listed for bank accounts used to operate Jetflicks. The email accounts identified as used to operate Jetflicks were accessed on a nearly daily basis for several months at the 2216 Tona Property. The affidavit also relies upon financial records, internet records, and electronic communications to connect the Defendant, the operation of Jetflicks, and the two residences. The Court finds that the affidavit shows a fair probability that contraband or evidence of a crime would be found in

defendant's properties from which he operated the alleged copyright endeavor. See United States v. Hill, 55 F.3d 479, 480 (9th Cir. 1995).

Accordingly, the Court finds that there was sufficient probable cause to support the warrant with respect to this email account.

ii. Lack of Sufficient Particularity

Mr. Dallmann argues that the search warrant was an unconstitutional general warrant because it lacked particularity. It thus allowed officers to conduct an exploratory search as there were no limits on what items could be seized.

As noted previously in this order, the Fourth Amendment's specificity requirement prevents officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized. United States v. Adjani, 452 F.3d 1140, 1147 (9th Cir. 2006) (citations omitted). The Ninth Circuit has determined that specificity is distinguished by two aspects – particularity and breadth.

Particularity is the requirement that the warrant must clearly state what is sought. United States v. SDI Future Health, Inc., 568 F.3d 684, 702 (9th Cir. 2009) (citing In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 856-57 (9th Cir. 1991)). Particularity means that "the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize." Id.

Here, the search warrant authorizes the seizure of records and information related to the alleged charges. It also identifies the type of evidence sought ("Records and information relating to the use of programs … to search, locate, download, process and store copyrighted TV shows, movies, and other works without the permission of the copyright owners") and where that information might be located ("All containers in which the items describe above may be stored"). The Court finds that the description is specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized. Id. (citing United States v. Smith, 424 F.3d 992, 1004 (9th Cir. 2005)).

Hence, the Court finds the search warrant did not lack probable cause or sufficient particularity. Accordingly, the Court finds that the search warrant is valid.

iii. Tainted by Other Fourth Amendment Violations

Mr. Dallmann argues that the evidence obtained from the search of the Tona Circle properties were obtained from search warrants that relied on inappropriately obtained information. For example, SA Chase used information received from Google to support his search warrant for the Defendant's properties.

Generally, evidence seized pursuant to an invalid warrant is subject to suppression under the exclusionary rule. See United States v. Henderson, 906 F.3d 1109, 1114-15 (9th Cir. 2018). The fruit of the poisonous tree doctrine is an extension of the exclusionary rule. Lingo v. City of Salem, 832 F.3d 953, 957-58 (9th Cir. 2016) ("The 'fruit of the poisonous tree' doctrine extends the exclusionary rule to require suppression of other evidence that is derived from—and is thus tainted by—the illegal search or seizure."). "[T]he exclusionary rule encompasses both the primary evidence obtained as a direct result of an illegal search or seizure and … evidence later discovered and found to be derivative of an illegality, the so-called fruit of the poisonous tree." Utah v. Strieff, 579 U.S. 232, 237 (2016) (quotation marks omitted).

As explained, the Court finds no basis to invalid the search warrants. Accordingly, the Court will not exclude evidence obtained from the discussed searches and seizures.

V. CONCLUSION

IT IS HEREBY ORDERED that the [ECF No. 157] Motion to Suppress is **DENIED**.

DATED: May 25, 2024

RICHARD F. BOULWARE, II
UNITED STATES DISTRICT JUDGE